Revista Universul Juridic ● nr. 7, iulie 2022, pp. 59-71

REGLEMENTAREA EXERCITĂRII PROFESIEI DE AUDITOR DE SECURITATE CIBERNETICĂ ÎN ROMÂNIA

Ramona CIOBANU
Universitatea Transilvania din Braşov
Facultatea de Drept

Abstract

The sharp digitalization of the last decade, in the private sector, but also in the public sector, have determined the special concern for the security of information systems, including by adopting legal rules to ensure the appropriate legal framework for conducting activities under the new conditions. In view of these trends, but also assuming its obligations as a member state of the European Union, Romania has established the National Cyber Security Strategy and the National Cyber Security Directorate, adopted legal rules for the security of computer networks and systems, for cyber security auditing and auditors. Regulation of March 22, 2021 for the attestation and verification of cyber security auditors, approved by Order no. 559/2021, adopted by the General Secretariat of the Government and published in the Official Monitor of Romania no. 387 of April 14, 2021, Part I, provides the regulatory framework for a professional, fair, objective and impartial audit. This normative act regulates the attestation, suspension and revocation of the cyber security auditor certificate, the conduct of auditors, its verification and the application of sanctions, as well as the evidence of the auditors through the National Register of Cyber Security Auditors. It should be noted that the Regulation applies only to the attestation and verification of cyber security auditors who ensure the audit of networks and computer systems that support essential services or provide digital services, while the cyber security audit at other institutions may be performed without this attestation, the existence of a certification of this specialization, issued by a trainer from the public or private sector, being sufficient.

Keywords: *computer systems, cyber security, cyber security auditor.*

1. Considerații introductive privind exercitarea profesiei de auditor de securitate cibernetică

Profesia de auditor al sistemelor informatice, pentru care se folosesc şi denumiri precum cea de *auditor informatic*, *auditor IT* sau *auditor de securitate cibernetică*, face parte din categoria profesiilor liberale.

Auditorul sistemelor informatice este un specialist cu cunoştinţe solide de informatică, care cunoaşte legislaţia specifică şi care are diplome, certificări şi autorizări recunoscute în domeniul auditului sistemelor informatice, documente care atestă că poate soluţiona probleme specifice sistemului informatic, poate parcurge etapele auditului informatic şi poate elabora raportul de audit[1].

Auditul sistemului informatic este o activitate complexă, care presupune verificarea, testarea, controlul specificaţiilor, aplicaţiilor, programelor, bazelor de date, dar şi a proceselor specifice ciclului de viaţă[2] ale unui program, aplicaţii, sistem informatic sau portal complex aparţinând entităţii auditate[3]. Obiectivul fundamental al acestui tip de audit îl constituie stabilirea gradului de credibilitate al soluţiilor de management al sistemului informatizat, scop în care auditorul va compara sistemul informatic auditat cu un sistem ideal.

Pentru a obţine o imagine cât mai exactă asupra activităţii entităţii auditate, auditorul va întreprinde o activitate de documentare cu privire la entitatea auditată, activitatea acesteia, domeniul în care-şi desfăşoară activitatea şi problemele specifice domeniului, legislaţia şi standardele aplicabile, aspecte legate de managementul organizaţiei şi managementul sistemului informatic, soluţii tehnice implementate, aspecte contractuale, activitatea de control şi audit informatic intern, auditurile IT anterioare şi concluziile acestora, activităţile de *follow up* desfăşurate şi, în general, orice aspecte care consideră auditorul că servesc îndeplinirii scopului auditului. Obţinând aceste informaţii, auditorul va putea evalua corect riscurile şi vulnerabilităţile sistemului informatic auditat, riscul de eroare şi/sau de fraudă, şi va fi în măsură să realizeze în mod adecvat planul şi programul de audit, va putea stabili corect strategia de audit, dar şi metoda de auditare.

Activitatea de audit se finalizează cu încheierea Raportului de audit, care cuprinde concluziile şi opinia auditorului, fundamentate pe probe. Orice afirmaţie a auditorului va trebui confirmată, susţinută de probele de audit. Acestea sunt obţinute pe parcursul misiunii de audit, auditorul folosind în acest sens toată experienţa şi cunoştinţele sale tehnice, în domeniul legislaţiei, standardelor, abilităţile organizatorice, dar şi abilităţi şi cunoştinţe care ţin de domeniul psihologiei dacă avem în vedere efortul de obţinere a informaţiilor relevante pentru audit. Astfel, pe lângă activităţile tehnice specifice auditului sistemelor informatice, auditorul va verifica toate documentele considerate utile pentru atingerea obiectivelor misiunii de audit, va cere, dacă este cazul, părerea unor specialişti din afara instituţiei auditate, va intervieva persoane din interiorul instituţiei care ar putea furniza

[1] Ion Ivan, Alecu Felician, Sergiu Capisizu, *Auditul informatic*, în Revista Economistul, 1887/2005, p. 2, http://alecu.ase.ro/articles/economistul_2005.pdf.

[2] A întregului ciclu de viaţă sau numai a unei secvenţe a acestuia.

[3] Pentru detalii privind auditul sistemelor informatice, a se vedea Ramona Ciobanu, *Tendinţe actuale în activitatea de audit. Auditul sistemelor informatice*, în Revista Universul Juridic nr. 2/2022, pp. 90-101, https://www.universuljuridic.ro/tendinte-actuale-in-activitatea-de-audit-auditul-sistemelor-informatice/.

informații utile, precum membrii echipei de management, auditori interni, managerii IT şi persoanele cu atribuții în administrarea, monitorizarea, întreținerea şi utilizarea sistemului informatic, utilizatori, alți angajați.

Literatura de specialitate, dar şi standardele recomandă ca auditorul să fie *rezervat* pe parcursul misiunii de audit, în relațiile cu personalul entității auditate, dar din practică rezultă că pentru succesul misiunii de audit comunicarea este vitală. Elemente ale comunicării, precum cuvintele (7%), timbrul vocii (38%), mimica, gestica, ținuta, contactul cu privirea (55%) sunt foarte importante[4]. Auditorul trebuie să fie rezervat, dar nu trebuie să construiască un zid între el şi personalul entității auditate, să se comporte şi să fie perceput ca un inamic, ci dimpotrivă trebuie să poarte discuții, să manifeste empatie, să creeze cadrul şi atmosfera propice pentru destăinuiri, să conducă dialogul cu persoanele din instituție de aşa manieră încât să obțină informații privitoare la activitatea entității auditate. Este vorba despre *tehnica ascultării active* pe care ar trebui să o stăpânească toți auditorii, apreciată de practicieni şi teoreticieni deopotrivă ca fiind cheia comunicării eficiente.

Comunicarea este una dintre cele mai importante aptitudini ale omului. Ea constă în vorbire, scriere şi ascultare. Ascultarea, ignorată de multe ori, nu este un demers facil, aşa cum ar părea la prima vedere. Ea necesită concentrare, o anumită atitudine, este un proces intelectual şi emoțional. Potrivit doctrinei[5] există patru categorii de persoane: non-ascultători, ascultători marginali, ascultători evaluatori şi ascultători activi, ascultarea activă fiind cea mai complexă formă de ascultare. Pentru desfăşurarea ascultării active trebuie luați în considerare trei factori: (1) aptitudinile de ascultare, (2) atitudinea ascultătorului şi (3) oportunitatea oferită de conversație[6].

Ascultarea activă presupune atenție completă la ceea ce spune interlocutorul, răbdare pentru a-l asculta fără a-l întrerupe, manifestarea interesului pentru cele relatate de vorbitor şi stimularea acestuia să se simtă important şi să vorbească, folosind în acest sens indicii verbale[7] ori non-verbale[8]. Ascultarea activă înseamnă a auzi mai mult decât spune interlocutorul, presupune desluşirea sensului ascuns al afirmațiilor acestuia sau, altfel spus, ce se află dincolo de cuvinte. De aceea,

---

[4] Ion Ivan, Alecu Felician, Sergiu Capisizu, *op. cit.*, p. 4.

[5] Pentru detalii, a se vedea Phillip L. Hunsaker, Anthony J. Alessandra, *The new art of managing people: person-to-person skills, guidelines, and techniques every manager needs to guide, direct, and motivate the team*, New York: Free Press, 2008.

[6] Vahid Kohpeima Jahromi ş. a., *Active listening: The key of successful communication in hospital managers*, în Electronic Phisician, March 2016, Volume: 8, Issue: 3, p. 2124,
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4844478/

[7] Spre exemplu, încurajarea verbală minimă (*Da?, Chiar?, Interesant!, Ei, bine?*) ori reflectarea conținutului şi a sentimentelor vorbitorului prin folosirea unor expresii verbale (*Spune-mi mai multe despre... Mă bucur să ascult dacă vrei să vorbeşti despre...).*

[8] Putem menționa în acest sens: postura atentă, expresia facială încurajatoare/empatică, menținerea contactului vizual, tăcere atentă.

auditorul va analiza nu numai ceea ce afirmă în mod expres interlocutorul, ci şi intenţia şi sentimentele acestuia.

Ascultarea activă este importantă pentru o serie de categorii profesionale, precum persoane cu funcţii de conducere, poliţişti, magistraţi, angajaţi ai serviciilor secrete, funcţionari ai serviciilor sociale, medici şi, nu în ultimul rând, auditori, inclusiv auditori de securitate cibernetică.

Aşa cum pe bună dreptate s-a afirmat în literatura de specialitate[9], auditorii nu sunt nici prieteni, nici duşmani, ci profesionişti care trebuie să identifice punctele slabe ale ariei auditate, astfel că prin remedierea acestora să se reducă riscurile la un nivel acceptabil, să crească securitatea şi credibilitatea sistemului informatic utilizat, cu efecte pozitive asupra activităţii entităţii auditate.

Succesul misiunii de audit este asigurat de întrunirea cumulativă a unor condiţii care privesc pregătirea profesională a auditorilor, certificarea şi atestarea lor, dar şi folosirea pe parcursul activităţii de audit a unor instrumente care să asigure precizie, rigoare şi rapiditate, după cum urmează:

- auditorii să fie persoane calificate în domeniul informatic,
- să existe organisme recunoscute de certificare/atestare a auditorilor,
- pentru efectuarea auditului să fie folosite tehnicile de audit asistate de calculator[10] *(Computer Assisted Audit Techniques – CAATs).*

2. Reglementarea profesiei de auditor de securitate cibernetică

Digitizarea şi digitalizarea[11] accentuată a unui număr din ce în ce mai mare de domenii de activitate, în sectorul privat, dar şi în cel public, tendinţa de generalizare a utilizării sistemelor de prelucrare automată a datelor, au determinat preocuparea pentru creşterea securităţii sistemelor informatice, inclusiv apariţia unui

[9] Ion Ivan, Alecu Felician, Sergiu Capisizu, *op. cit.*, p. 4.

[10] Digitalizarea accentuată, volumul mare de date stocate la nivelul la nivelul instituţiilor, concurenţa economică acerbă impun necesitatea unor instrumente de audit care să corespundă cerinţelor utilizatorilor, precum acces şi procesare rapidă, siguranţa operaţiunilor, securitatea datelor, protecţie împotriva dezastrelor. Tehnicile clasice de audit trebuie dublate de tehnici noi, corespunzătoare noilor tendinţe şi nevoi, acesta fiind cadrul în care s-a impus utilizarea tehnicilor de audit asistate de calculator sau, pe scurt, *CAATs*. Potrivit Standardelor internaţionale de audit, CAATs reprezintă tehnici folosite de auditorii care utilizează calculatorul ca instrument pentru culegerea şi analiza datelor necesare auditului. De altfel, având în vedere caracteristicile noii economii, din ce în ce mai digitalizată, este aproape imposibil ca auditorii să colecteze probe de audit fără un instrument software de analiză a datelor. Se foloseşte *software-ul generalizat de audit (Generalized Audit Software – GAS)* şi *software-uri specializate*, precum testul de date, testul integrat, tehnici pentru analiza fluxurilor de date şi sisteme expert. Pentru detalii, a se vedea P. Năstase (coordinator) ş.a., *Auditul şi controlul sistemelor informaţionale*, Ed. Economică, Bucureşti, 2007, pp. 40-44.

[11] Pentru explicaţii privind noţiunile de digitizare, digitalizare, revoluţie digitală şi economie digitală, a se vedea Ramona Ciobanu, *Revoluţia digitală şi impozitarea*, în Curierul judiciar nr. 3/2021, pp. 127-132.

nou tip de audit: auditul sistemelor informatice. Necesitatea reducerii riscurilor inerente folosirii sistemelor informatice a impus pe lângă găsirea unor soluții tehnice şi adoptarea unor norme juridice noi, adecvate noilor realități, care să incrimineze fraudele informatice şi să combată criminalitatea cibernetică[12], să stabilească strategii naționale privind securitatea cibernetică şi obligațiile instituțiilor digitalizate privind creşterea gradului de securitate cibernetică, să reglementeze exercitarea profesiei de auditor de securitate cibernetică, inclusiv coduri etice aplicabile acestora.

România nu putea rămâne în afara acestui proces şi, chiar dacă paşii în sensul digitalizării pot fi considerați timizi în comparație cu stadiul la care au ajuns alte state, țara noastră urmează tendința prevalentă la nivel mondial. Pe de altă parte, calitatea României de stat membru al Uniunii Europene presupune obligații în privința digitalizării[13] şi asigurării securității cibernetice[14]. În consecință, au fost adoptate o serie de acte normative menite să armonizeze legislația românească cu cea europeană şi să creeze cadrul juridic necesar folosirii în condiții de siguranță a sistemelor informatice[15].

Cadrul legal pentru exercitarea profesiei de auditor de securitate cibernetică este *Regulamentul din 22 martie 2021 pentru atestarea şi verificarea auditorilor de securitate cibernetică, aprobat prin Ordinul nr. 559/2021*, adoptat de Secretariatul

---

[12] Potrivit notei finale nr. 5 din *Comunicarea comună către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor. Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur şi securizat /* JOIN/2013/01 final */*, „*criminalitatea cibernetică* se referă în general la o gamă largă de activități infracționale, care au ca instrument principal ori ca țintă principală calculatoarele şi sistemele informatice. Criminalitatea cibernetică include infracțiunile tradiționale (de exemplu frauda, falsificarea şi furtul de identitate), infracțiunile legate de conținut (de exemplu, distribuirea de pornografie infantilă sau instigarea la ură rasială online) şi infracțiunile asociate exclusiv calculatoarelor şi sistemelor informatice (de exemplu, atacurile împotriva sistemelor informatice, blocarea accesului şi malware-ul)", https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:52013JC0001.

[13] A se vedea, în acest sens, European Commision, *Europe's Digital Decade: Digital targets for 2030,* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

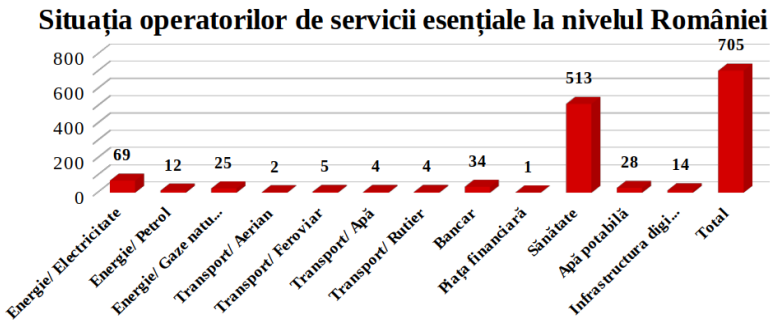
[14] A se vedea, în acest sens, *Rezoluția Parlamentului European din 10 iunie 2021 referitoare la Strategia de securitate cibernetică a UE pentru deceniul digital (2021/2568(RSP))*, publicată în Jurnalul Oficial al Uniunii Europene nr. C-67 din 8 februarie 2022, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.C_.2022.067.01.0081.01.RON&toc=OJ%3AC%3A2022%3A067%3ATOC; Directoratul Național de Securitate Cibernetică, *Noua strategie de securitate cibernetică a UE pentru Deceniul Digital şi impactul său pentru România*, https://dnsc.ro/citeste/noua-strategie-de-securitate-cibernetica-a-ue-pentru-deceniul-digital-si-impactul-sau-pentru-romania.

[15] Menționăm, în acest sens, H.G. nr. 271/2013 pentru aprobarea Strategiei de Securitate Cibernetică a României (SNSC) şi a Planului de acțiune la nivel național privind implementarea SNSC; Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice, denumită şi Legea NIS, lege care transpune în legislația internă Directiva UE 2016/1148 (NIS – Network and Information Security) a Parlamentului European şi a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor şi a sistemelor informatice în UE; O.U.G. nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică.

general al Guvernului şi publicat în Monitorul Oficial al României nr. 387 din 14 aprilie 2021, Partea I, pentru care vom folosi în continuare denumirea de *Regulament*, act normativ care reglementează atestarea, suspendarea şi revocarea atestatului de auditor de securitate cibernetică, desfăşurarea activităţii auditorilor şi a misiunii de audit, verificarea activităţii auditorilor de securitate cibernetică şi aplicarea sancţiunilor, evidenţa auditorilor prin Registrul Naţional al Auditorilor de Securitate Cibernetică.

Regulamentul se aplică pentru atestarea şi verificarea auditorilor de securitate cibernetică care asigură *auditarea reţelelor şi sistemelor informatice ce susţin servicii esenţiale ori furnizează servicii digitale*, în condiţiile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare, denumită şi Legea NIS [art. 1 alin. (1) din Regulament]. Potrivit art. 6 alin. (1) din Legea NIS, *un serviciu este considerat esenţial* dacă furnizarea lui îndeplineşte cumulativ următoarele condiţii: serviciul este esenţial în susţinerea unor activităţi societale şi/sau economice de cea mai mare importanţă; furnizarea sa depinde de o reţea sau de un sistem informatic; furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident. De asemenea, potrivit art. 3 lit. o) din Legea NIS, *furnizorul de servicii digitale* este orice entitate care furnizează servicii care se încadrează într-una din următoarele categorii: piaţă online, motor de căutare online, serviciu de cloud computing.

Potrivit Directoratului Naţional de Securitate Cibernetică (DNSC), sunt furnizori de servicii esenţiale operatorii din domeniul energiei (electricitate, petrol, gaze naturale), transport (aerian, feroviar, rutier, naval), bancar, piaţă financiară, sănătate, apă potabilă şi infrastructură digitală[16].



Sursa: Directoratul Naţional de Securitate Cibernetică, https://dnsc.ro/pagini/operatori-de-servicii-esentiale

[16] Evidenţa operatorilor de servicii esenţiale este asigurată de DNSC, respectiv Autoritatea competentă la nivel naţional pentru securitatea reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale ori furnizează serviciile digitale (ANSRSI), în Registrul Operatorilor de Servicii Esenţiale (OSE), registru care face parte din categoria documentelor clasificate, din clasa Secrete de Serviciu, https://dnsc.ro/pagini/operatori-de-servicii-esentiale.

Pentru celelalte domenii de activitate, auditorul de securitate cibernetică nu trebuie să fie atestat de DNSC, fiind suficientă existența unei certificări a acestei specializări, emisă de un formator din sectorul public sau privat[17].

Auditorul de securitate cibernetică este, potrivit art. 2 alin. (2) lit. a) din Regulament, persoana fizică atestată sau persoana juridică cu personal atestat „care realizează activități de auditare a rețelelor şi sistemelor informatice ce susțin servicii esențiale sau furnizează servicii digitale, conform reglementărilor şi bunelor practici în domeniu". Aşadar, profesia de auditor de securitate cibernetică poate fi exercitată de *persoane fizice atestate* să exercite activități specifice auditului de securitate cibernetică, respectiv activități „prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecție implementate la nivelul rețelelor şi sistemelor informatice, în vederea identificării disfuncțiilor şi vulnerabilităților şi a furnizării unor soluții de remediere a acestora [art. 2 alin. (2) lit. b) din Regulament], activități pe care le exercită în mod independent sau ca angajați ai unor *persoane juridice atestate,* la rândul lor, să desfăşoare atare activități.

3. Atestarea auditorilor de securitate cibernetică

Potrivit Regulamentului, atestarea auditorilor de securitate cibernetică se realizează de către Centrul Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO, în calitate de autoritate competentă la nivel național. *Regulamentul pentru atestarea şi verificarea auditorilor de securitate cibernetică* a fost adoptat, aşa cum am precizat mai sus, la data de 22 martie 2021 şi prevedea că CERT-RO este autoritatea competentă să autorizeze şi să verifice îndeplinirea obligațiilor profesionale de către auditorii de securitate cibernetică. La data de 17 septembrie 2021, la nici 6 luni de la actul normativ inițial, a fost adoptată Ordonanța de Urgență a Guvernului nr.104/2021 privind înființarea *Directoratului Național de Securitate Cibernetică (DNSC)* ca organ de specialitate al administrației publice centrale, în subordinea Guvernului şi în coordonarea prim-ministrului, cu personalitate juridică, finanțat integral din bugetul de stat, prin bugetul Secretariatului General al Guvernului, *având responsabilități privind securitatea cibernetică a spațiului cibernetic național civil.* CERT-RO s-a desființat la data intrării în vigoare a acestei ordonanțe de urgență, iar DNSC a preluat activitățile, atribuțiile şi personalul CERT-RO, inclusiv atribuțiile de atestare şi verificare a exercitării auditului de securitate cibernetică, domeniu în care este acum *autoritate competentă la nivel național.*

[17] Un auditor de securitate cibernetică poate deține şi alte atestate şi certificări, inclusiv de audit de securitate cibernetică, şi care nu fac obiectul Regulamentului.

Există trei categorii de atestate, astfel încât o *persoană fizică sau juridică poate solicita obținerea unuia dintre următoarele atestate:*

a) *atestat tip general:* pentru toate activitățile de audit, speciale şi comune

b) *atestat tip special:* numai pentru activitățile de audit speciale şi anume auditul codului de sursă şi auditul de penetrare şi testarea de penetrare

c) *atestat tip comun:* numai pentru activitățile de audit comune şi anume auditul arhitecturii, auditul de configurare şi auditul securității organizației.

Atestatul de auditor de securitate cibernetică se obține în baza cererii pentru emiterea atestatului de auditor de securitate cibernetică şi a dosarului pentru emiterea atestatului de auditor de securitate cibernetică.

Dosarul pentru emiterea *atestatului de auditor de securitate cibernetică pentru o persoană fizică* trebuie să cuprindă următoarele documente:

a) actul de identitate, în copie

b) adeverința medicală din care să rezulte starea de sănătate fizică şi psihică a solicitantului pentru exercitarea atribuțiilor de auditor de securitate cibernetică

c) certificatul de cazier judiciar, aflat în termenul de valabilitate

d) curriculum vitae – model europass, cu detalierea secțiunii „experiență profesională" ce va conține justificarea privind experiența în domeniu, respectiv cele care prezintă dovada a cel puțin 2 ani de experiență în domeniul administrării sau implementării rețelelor şi sistemelor informatice *sau* 2 ani de experiență în domeniul securității rețelelor şi sistemelor informatice sau un an de experiență în domeniul investigațiilor, testării *sau* al auditului de securitate a tehnologiei informației şi comunicațiilor sau a rețelelor şi sistemelor informatice ori a sistemelor de control industrial

e) certificări[18], în copii – în funcție de tipul de atestat solicitat:

- *atestare tip general* – cel puțin două dintre certificările profesionale menționate în Anexa nr. 5 a Regulamentului (dintre care cel puțin una dintre activitățile de audit comune şi cel puțin una dintre activitățile de audit speciale), în perioada de valabilitate;
- *atestare tip special* – cel puțin una dintre certificările profesionale pentru activitățile de audit speciale menționate în Anexa nr. 5 a Regulamentului, în perioada de valabilitate;
- *atestare tip comun* – cel puțin una dintre certificările profesionale pentru activitățile de audit comune menționate în Anexa nr. 5 a Regulamentului, în perioada de valabilitate *sau certificat evaluare expertiză privind securitatea cibernetică* eliberat de către autoritatea competentă național.

[18] Anexa 5 a Regulamentului cuprinde 37 de certificări. Aceasta va fi actualizată/completată permanent, ştiut fiind că domeniul tehnologiei informației este caracterizat printr-o dinamică accentuată, şi publicată pe site-ul DNSC; a se vedea Anexa 5: LISTA CERTIFICĂRILOR PROFESIONALE din Regulamentul din 22 martie 2021 pentru atestarea şi verificarea auditorilor de securitate cibernetică.

f) certificatul de specializare de auditor de securitate cibernetică valabil[19], eliberat de un formator sau furnizor de servicii de formare *autorizat* de către autoritatea competentă la nivel național[20];

g) taxa de evaluare şi procesare (PF) în vederea atestării ca auditor de securitate cibernetică.

Dosarul pentru emiterea atestatului de auditor de securitate cibernetică pentru o persoană juridică trebuie să cuprindă următoarele documente:

a) documentul de înființare/înregistrare al persoanei juridice, respectiv certificat de înregistrare în registrele naționale (Registrul Comerțului);

b) certificat constatator emis de instituția care gestionează registrul în care se ține evidența înființării persoanei juridice, cu starea la zi a persoanei juridice, nu mai vechi de 30 de zile, în original sau în copie semnată şi cu mențiunea „conform cu originalul";

c) documentele doveditoare pentru fiecare auditor de securitate cibernetică persoană fizică;

d) taxa de evaluare şi procesare (PJ) în vederea atestării ca auditor de securitate cibernetică.

Dosarul pentru emiterea atestatului de auditor de securitate cibernetică se depune împreună cu cererea de emitere a atestatului de auditor de securitate cibernetică la autoritatea competentă la nivel național care va desfăşura procedura de evaluare şi atestare a auditorului de securitate cibernetică potrivit dispozițiilor art. 8-13 din Regulament.

---

[19] Trebuie să facem distincție între:

- *Atestatul de auditor de securitate cibernetică* emis de Directoratul Național de Securitate Cibernetică care dă dreptul de a efectua misiuni de audit potrivit Regulamentului şi Legii NIS;
- *Certificatul de specializare de auditor de securitate cibernetică* eliberat de un formator sau furnizor de servicii de formare autorizat de către Directoratul Național de Securitate Cibernetică, existența acestei certificări fiind o condiție obligatorie pentru obținerea calității de auditor de securitate cibernetică *atestat* de DNSC;
- *Certificatul de specializare de auditor de securitate cibernetică* eliberat în alte condiții decât cele prevăzute în Regulament şi care-i dă dreptul titularului să efectueze auditul de securitate cibernetică la alte entități decât cele prevăzute în Regulament;
- *Certificat evaluare expertiză* emis de DNSC şi care trebuie obținut dacă aspirantul la atestatul de auditor de securitate cibernetică aplică pentru atestatul de tip comun şi nu are cel puțin una din certificările din Anexa 5 a Regulamentului; pentru obținerea lui trebuie urmată procedura prevăzută de Regulament.

[20] Potrivit art. 36 alin. (1) din Regulament, în procesul de eliberare a atestatului de auditor de securitate cibernetică, lipsa certificatul de specializare de auditor de securitate cibernetică, eliberat de un formator sau furnizor de servicii de formare *autorizat* de către Directoratul Național de Securitate Cibernetică, va fi acceptată până la data publicării Listei formatorilor şi furnizorilor de servicii de formare pentru auditorii de securitate cibernetică pe site-ul instituției, dată de la care va avea un termen de 6 luni pentru finalizarea cursului şi transmiterea DNSC a copiei certificatului de specializare (art. 36 alin. 2 din Regulament). Până în prezent, această listă nu a fost publicată pe site-ul instituției, secțiunea fiind în lucru; a se vedea https://dnsc.ro/pagini/formatori-si-furnizori-de-servicii-de-formare.

Autoritatea competentă la nivel național întocmeşte *raportul final de evaluare* prin care se propune emiterea atestatului de auditor de securitate cibernetică sau restituirea dosarului. În baza raportului final de evaluare, autoritatea competentă la nivel național emite atestatul de auditor de securitate cibernetică, ia în evidență auditorul de securitate cibernetică şi actualizează lista auditorilor de securitate cibernetică.

Evidența auditorilor de securitate cibernetică se ține de către autoritatea competentă la nivel național, DNSC, în format electronic, pe baza *Registrului național al auditorilor de securitate cibernetică.* Registrul se constituie în format electronic pe variantele de atestare prezentate (persoane fizice şi juridice) şi cuprinde date şi informații cu privire la auditorii de securitate cibernetică atestați, revocați sau suspendați din profesia de auditor de securitate cibernetică. În baza Registrului național al auditorilor de securitate cibernetică, DNSC elaborează, actualizează în permanență şi publică pe site-ul instituției Lista auditorilor de securitate cibernetică persoane fizice şi persoane juridice[21].

4. Reînnoirea, revocarea şi suspendarea atestatului de auditor de securitate cibernetică

Reînnoirea atestatului. Atestatul are o valabilitate de 3 ani, fiind posibilă reînnoirea acestuia potrivit dispozițiilor art. 15 din Regulament care reglementează procedura de reînnoire. Astfel, cu 60 de zile înainte de expirarea termenului de valabilitate a atestatului, auditorul de securitate cibernetică va solicita DNSC reînnoirea atestatului, înaintând în acest sens cererea şi dosarul de reînnoire a atestatului.

Revocarea şi suspendarea atestatului. În cazul nerespectării de către auditor a obligațiilor prevăzute în Regulament, Legea NIS sau alte acte normative, autoritatea competentă la nivel național va revoca[22] sau suspenda[23] atestatul, după caz.

5. Principiile aplicabile profesiei de auditor de securitate cibernetică

În desfăşurarea activității specifice de audit, auditorul de securitate cibernetică este obligat să respecte principiile fundamentale prevăzute la art. 6 din Codul etic al auditorului de securitate cibernetică şi anume: *integritatea, independența, obiectivitatea, confidențialitatea, competența profesională şi neutralitatea politică.* Aceste principii sunt în acord cu principiile stabilite de-a lungul timpului de organizațiile

[21] La data ultimei actualizări a celor două liste, 24.05.2022, existau 90 de auditori de securitate cibernetică persoane fizice (https://dnsc.ro/vezi/document/lista-aasc-pf) şi 42 de auditori de securitate cibernetică persoane juridice (https://dnsc.ro/vezi/document/lista-aasc-pj).

[22] Procedura revocării atestatului este reglementată de art. 14 din Regulament.

[23] Procedura suspendării atestatului este reglementată de art. 16 din Regulament.

profesionale ale auditorilor pe plan internațional, inclusiv de cele ale auditorilor sistemelor informatice, principii al căror rol este acela de a călăuzi activitatea auditorilor şi de a asigura corectitudinea, obiectivitatea, profesionalismul şi imparțialitatea pe parcursul misiunii de audit, dar şi păstrarea secretului profesional de către auditori. Codul etic al auditorului de securitate cibernetică, reglementat în Anexa 13 a Regulamentului, stabileşte conținutul principiilor fundamentale, oferind interpretarea legală a acestora.

6. Obligațiile auditorului de securitate cibernetică

Obligația de respectare a Codului etic. Regulamentul prevede obligațiile auditorului de securitate cibernetică la Capitolul III, intitulat *Condiții şi cerințe pentru auditorii de securitate cibernetică.* Printre obligațiile reglementate de Regulament o regăsim şi pe cea de respectare a *Codului etic al auditorului de securitate cibernetică* (art. 20 alin. 1), ca ansamblu de principii şi reguli de conduită care trebuie să guverneze activitatea auditorului de securitate cibernetică.

Astfel, în maximum 10 zile de la obținerea atestatului de auditor de securitate cibernetică, auditorul va lua act de Codul etic şi va semna, olograf sau digital, declarația/angajamentul privind respectarea Codului etic al auditorului de securitate cibernetică, folosind formularul din Regulament[24]. Declarația va fi transmisă autorității competente la nivel național (art. 20 alin. 2). Nesemnarea şi/sau netransmiterea declarației/ angajamentului duce, după caz, la suspendarea atestatului după a 11-a zi de la emiterea atestatului, dar nu mai mult de 30 de zile sau la revocarea după cea de a 31-a zi de la emiterea atestatului (art. 20 alin. 3).

Codul etic al auditorului de securitate cibernetică reglementează şi el la Capitolul III, intitulat *Reguli de conduită*, obligații pentru auditor.

Obligația de raportare a auditorilor către autoritatea competentă. Anual, în primul trimestru, auditorii de securitate cibernetică vor transmite la autoritatea competentă la nivel național, în format electronic, un raport/o situație a auditurilor de securitate desfăşurate în anul calendaristic precedent, cu precizarea numărului, beneficiarilor, perioadelor, neregulilor grave constatate, precum şi a şi vulnerabilităților constatate, conform modelului din Anexa 11 a Regulamentului.

Alte obligații. Anexa 6 a Regulamentului, intitulată *Abilități, aptitudini şi acțiuni specifice auditorilor de securitate cibernetică*, aduce un plus de exigență profesiei de auditor, prevăzând şi ea obligații pentru acesta.

---

[24] A se vedea *Declarația/ angajamentul privind respectarea Codului etic al auditorului de securitate cibernetică, https://dnsc.ro/vezi/document/anexa-nr-13-modelul-de-declaratie-angajament-privind-respectarea-cod-etic-asc.*

7. Verificarea activității auditorilor de securitate cibernetică. Sancțiuni

Autoritatea competentă la nivel național, DNSC, verifică modul de îndeplinire a activității de către auditorii de securitate cibernetică, în baza planului de control anual, a sesizărilor primite sau a activității de monitorizare a aplicării prevederilor Legii NIS la nivelul României.

DNSC verifică, în urma sesizărilor primite sau din oficiu, îndeplinirea de către auditorii de securitate cibernetică a obligațiilor legale care le revin şi poate dispune, dacă este cazul, următoarele măsuri:

- remedierea deficiențelor constatate,
- suspendarea activității pe o perioadă specificată,
- revocarea atestatului de auditor de securitate cibernetică.

Concluzii

Extinderea utilizării sistemelor informatice în economie, administrație, sănătate, învățământ, dar şi în alte domenii, prezența şi aproape *dependența* de sistemele informatice în viața de zi cu zi impun găsirea unor soluții tehnice menite să sporească gradul de securitate a sistemelor şi rețelelor informatice, precum şi controlul eficienței acestor soluții, identificarea vulnerabilităților şi corectarea lor. În acest efort se înscrie şi activitatea auditorilor de securitate cibernetică, profesie cu o existență de câteva decenii în statele dezvoltate şi relativ nouă în celelalte. Dacă avem în vedere pericolele care pândesc instituțiile digitalizate, printre care enumerăm alterarea şi pierderea datelor ori deconspirarea acestora ca urmare a criminalității cibernetice, din ce în ce mai agresivă şi mai organizată, iată o nouă formă de manifestare a criminalității organizate cu caracter transfrontalier, putem conchide că activitatea auditorilor de securitate cibernetică va fi în viitor la fel de necesară ca cea a auditorilor financiari, spre exemplu.

Datorită avantajelor pe care le procură digitalizarea, statele au stabilit strategii de extindere a acesteia, dar pentru că ea are riscuri asociate importante, statele sunt nevoite să pună la punct şi strategii de securitate cibernetică.

România a fost mereu atentă la tendințele manifestate pe plan mondial, astfel încât şi de această dată întreprinde măsuri pentru asigurarea securității cibernetice, inclusiv prin activitatea auditorilor de securitate cibernetică, a căror atestare şi exercitare a activității a reglementat-o, deocamdată pentru auditul desfăşurat la operatorii care furnizează servicii esențiale ori furnizează serviciile digitale.

Bibliografie

1. Ramona Ciobanu, *Tendințe actuale în activitatea de audit. Auditul sistemelor informatice*, în Revista Universul Juridic nr. 2/2022, https://www.universuljuridic.ro/tendinte-actuale-in-activitatea-de-audit-auditul-sistemelor-informatice/.

2. Ramona Ciobanu, *Revoluția digitală şi impozitarea*, în Curierul judiciar nr. 3/2021.

3. Comisia Europeană, *Comunicarea comună către Parlamentul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor. Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur şi securizat /* JOIN/2013/01 final */,* https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:52013JC0001.

4. Comisia Europeană, *Europe's Digital Decade: Digital targets for 2030,* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

5. Directoratul Național de Securitate Cibernetică, *Noua strategie de securitate cibernetică a UE pentru Deceniul Digital şi impactul său pentru România*, https://dnsc.ro/citeste/noua-strategie-de-securitate-cibernetica-a-ue-pentru-deceniul-digital-si-impactul-sau-pentru-romania.

6. Directoratul Național de Securitate Cibernetică, *Operatori de servicii esențiale*, https://dnsc.ro/pagini/operatori-de-servicii-esentiale.

7. Directoratul Național de Securitate Cibernetică, *Formatori şi furnizori de servicii de formare*, https://dnsc.ro/pagini/formatori-si-furnizori-de-servicii-de-formare.

8. Phillip L. Hunsaker, Anthony J. Alessandra, *The new art of managing people: person-to-person skills, guidelines, and techniques every manager needs to guide, direct, and motivate the team*, New York: Free Press, 2008.

9. Ion Ivan, Alecu Felician, Sergiu Capisizu, *Auditul informatic*, în Revista Economistul, 1887/2005, http://alecu.ase.ro/articles/economistul_2005.pdf.

10. Vahid Kohpeima Jahromi ş. a., *Active listening: The key of successful communication in hospital managers*, în Electronic Phisician, March 2016, Volume: 8, Issue: 3,
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4844478/.

11. P. Năstase (coordonator) ş.a., *Auditul şi controlul sistemelor informaționale*, Ed. Economică, Bucureşti, 2007.

12. Parlamentul European, *Rezoluția din 10 iunie 2021 referitoare la Strategia de securitate cibernetică a UE pentru deceniul digital (2021/2568(RSP))*, publicată în Jurnalul Oficial al Uniunii Europene nr. C-67 din 8 februarie 2022, https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.C_.2022.067.01.0081.01.RON&toc=OJ%3AC%3A2022%3A067%3ATOC.